

BOLLETTINO DI SICUREZZA XEROX XRX08-001

Il controller di rete/ESS presenta vulnerabilità che, se sfruttate, potrebbero consentire l'esecuzione in remoto di codici arbitrari tramite richieste RPC (Remote Procedure Call) designate allo scopo.

Si forniscono qui sotto una soluzione software (patch P32) e le istruzioni per installarla sui prodotti indicati. La patch è stata creata in modo che possa essere installata direttamente dal cliente. La soluzione software è disponibile come file ZIP di 8.3 MB dal collegamento riportato qui sotto:

http://www.xerox.com/downloads/usa/en/c/cert_P32v2_WCP275_WC7665_Patch.zip

La patch P32 è classificata come patch **importante**.

L'installazione della patch è particolarmente raccomandata ai clienti preoccupati della vulnerabilità dei prodotti elencati di seguito. Tuttavia, leggere prima le istruzioni di installazione allegate per controllare di disporre della versione adeguata per l'installazione.

- Per i prodotti della serie WorkCentre®/WorkCentre® Pro 2xx, il software di sistema versione *.60.22.007 o superiore (controller ESS versione 040.022.x1110 o superiore) contiene già questa correzione e pertanto la patch è superflua.
- Per i prodotti WorkCentre® 7655/7665, il software di sistema versione 040.032.55080 o superiore (controller ESS versione 040.032.55080 o superiore) contiene già questa correzione e pertanto la patch è superflua. Inoltre, per WorkCentre® 7655/7665, se il software di sistema non è 040.032.53080 o superiore (controller di rete versione 040.022.*1031 o superiore), occorre contattare l'assistenza tecnica per eseguire l'aggiornamento della macchina al software di sistema/controller di rete versione 040.032.53080, prima di applicare la patch.

Nota: questa patch di sicurezza è contrassegnata dal codice **P32**. Una volta installata la patch correttamente, la versione del controller di rete avrà il suffisso **.P32** (ad esempio, 040.022.x0115.P32).

Rischio

Nell'ambito dei controlli costanti per proteggere i clienti da potenziali attacchi, Xerox ha scoperto le seguenti vulnerabilità:

- CVE-2007-2446 - Sovraccarichi di heap multipli permettono l'esecuzione in remoto di codici non autorizzati
- CVE-2007-2447 - Vulnerabilità di tipo "command injection" in remoto

Queste vulnerabilità, presenti nel codice del controller di rete/ESS che gestisce i servizi di condivisione di file e stampanti per i client SMB/CIFS (Service Message Block/Common Internet File System) quali i dispositivi MFD Xerox, potrebbero consentire l'esecuzione in remoto di codici arbitrari tramite richieste RPC (Remote Procedure Call) designate allo scopo. Le vulnerabilità colpiscono solo i servizi di condivisione delle stampanti. Un pirata informatico potrebbe apportare modifiche non autorizzate alla configurazione del sistema. Tuttavia, le password di clienti e utenti non sono a rischio.

Questa patch si applica solo ai modelli connessi in rete¹ dei seguenti prodotti:

| WorkCentre® | WorkCentre Pro® |
|-------------|-----------------|
| 232 | 232 |
| 238 | 238 |
| 245 | 245 |
| 255 | 255 |
| 265 | 265 |
| 275 | 275 |
| 7655 | |
| 7665 | |

¹Se il prodotto non è collegato alla rete, non è vulnerabile agli attacchi, pertanto non è richiesta alcuna azione preventiva.

Soluzione

Istruzioni di installazione

Nome file della patch: **WCP275_WC7665_P32v2.dlm**

La patch può essere installata sul sistema seguendo le istruzioni riportate di seguito.

Riepilogo delle versioni e delle procedure:

- Stabilire la versione iniziale del software di sistema o la versione del controller ESS
- Stabilire quali sono gli aggiornamenti necessari
- Eseguire l'aggiornamento dei dispositivi in base alle esigenze
- Applicare la patch, se necessario

Per WC/WCP 232/238/245/255/265/275

| | Se la versione del software è SW sistema o Controller ESS | | Installare la patch? | Passaggio successivo: | Quindi: | Nuovo numero del controller di rete/ESS: |
|---|-----------------------------------------------------------|-------------------------------------|----------------------|----------------------------------------------------------------------------------------------|-----------------------|-------------------------------------------------------------|
| 1 | Da *.27.24.000 a *.27.24.020 | Da 040.010.#0930 a 040.010.#1160 | No | Eseguire l'aggiornamento o a *.60.22.000 o versione successiva. Vedere l'Appendice A | Caricare la patch P32 | 040.022.#1031.BIOSxx.xx.P32v2 |
| 2 | Da *.50.03.000 a *.50.03.009 | Da 040.010.#1172 a 040.010.#2250 | No | Eseguire l'aggiornamento o a *.60.22.000 o versione successiva. Vedere l'Appendice A | Caricare la patch P32 | 040.022.#1031.BIOSxx.xx.P32v2 (se la patch viene applicata) |
| 3 | *.50.03.011 | 040.010.#2280 | No | Rivolgersi all'assistenza per eseguire l'aggiornamento o a *.60.22.000 o versione successiva | Caricare la patch P32 | 040.022.#1031.BIOSxx.xx.P32v2 (se la patch viene applicata) |
| 4 | *.27.24.015 (con certificazione Common Criteria) | 040.010.#1121 | No | Vedere la NOTA 1 di seguito | - | - |
| 5 | *.39.24.001 (Certificazione Common Criteria) | 040.010.#1123 | No | Vedere la NOTA 1 di seguito | - | - |
| 6 | *.60.15.000 | 040.022.#0112 | No | Eseguire l'aggiornamento o alla versione *.60.22.000 o superiore. Vedere l'Appendice A | Caricare la patch P32 | 040.022.#1031.BIOSxx.xx.P32v2 |
| 7 | *.60.17.000 (con certificazione Common Criteria) | 040.022.#0115 | Si | Vedere la NOTA 1 di seguito | - | 040.022.#0115.P32v2 (se la patch viene applicata) |

| | | | | | | |
|---|---------------------------------|-------------------------------------|-----|--------------------------|---|---------------------------------------------------------------------------|
| 8 | Da *.60.17.000 a *.60.22.006 | Da 040.022.#0115 a 040.022.#1100 | Sì | Caricare la patch P32 | - | Da 040.022.#0115.BIOSxx.xx.P32v2 a 040.022.#1100.BIOSxx.xx.P32v2 |
| 9 | *.60.22.007 e superiore | 040.022.#1100 o superiore | N/A | Fatto | - | - |

NOTA 1: se la versione del software di sistema è *.27.24.015, *.39.24.001 o 60.17.000, il dispositivo dispone di una certificazione Common Criteria. Se la versione del software di sistema è inferiore, è possibile eseguire l'aggiornamento alla versione *.60.17.000 e successivamente caricare la patch P32. A questo punto tuttavia il dispositivo non disporrà più della certificazione Common Criteria.

Per WC 7655/7665

| | Se la versione del software è SW sistema o Controller di rete | | Installare la patch? | Passaggio successivo: | Quindi: | Nuovo numero del controller di rete/ESS: |
|---|------------------------------------------------------------------|----------------------------------------|-------------------------|---------------------------------------------------------------------------------------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|
| 1 | Da 040.032.50855 a 040.032.51040 | Da 040.032.50855 a 040.032.51030 | No | Rivolgersi all'assistenza tecnica per eseguire l'aggiornament o alla versione 040.032.53080 | Caricare la patch P32 | 040.032.53080.BIOSxx.xx.P32v2 |
| 2 | 040.032.53080 | 040.032.53080 | Sì | Caricare la patch P32 | - | 040.032.53080.BIOSxx.xx.P32v2 |
| 3 | 040.032.53080 con certificazione Common Criteria | 040.032.53080 | Sì | Vedere la NOTA 1 di seguito | - | 040.032.53080.BIOSxx.xx.P32v2 (se la patch viene applicata) |
| 4 | Da 040.032.55030 a 040.032.55070 | Da 040.032.55030 a 040.032.55070 | Sì | Vedere la NOTA 1 di seguito | - | Da 040.032.55030.BIOSxx.xx. P31v14 a 040.032.55060.BIOSxx.xx. P31v14 (se la patch viene applicata) |
| 5 | 040.032.55080 e superiore | 040.032.55080 | N/A | Fatto | - | - |

NOTA 1: se la versione del software di sistema è 040.032.53080, il dispositivo dispone di una certificazione Common Criteria. Se lo si desidera, si può caricare la patch P32, tuttavia così facendo si invaliderà la certificazione Common Criteria.

Installazione della patch

È necessario innanzitutto scaricare la patch. La patch è compressa in formato ZIP. Scaricare il file ZIP dall'URL indicato ed estrarre tutto il contenuto sul desktop. Non tentare di aprire il file con estensione .DLM: si tratta della patch e deve essere installata sul dispositivo multifunzione così com'è.

Metodi di installazione della patch

La patch di aggiornamento (come la maggior parte del software) può (e deve) essere installata dal cliente. È possibile eseguire l'installazione seguendo vari metodi.

- Metodo Software macchina (Aggiornamento): inviare un file di aggiornamento/patch al dispositivo utilizzando la pagina Web del dispositivo
- Comando LPR: applicare l'aggiornamento/patch a un singolo dispositivo utilizzando un comando LPR.
- Batch di comandi LPR: applicare l'aggiornamento/patch a vari dispositivi utilizzando un batch di comandi LPR.
- XDM e CenterWare Web: inviare i file di aggiornamento/patch a vari dispositivi tramite XDM e CenterWare Web.

Per ulteriori informazioni sui metodi riportati sopra, vedere il suggerimento "How to Upgrade, Patch or Clone Xerox Multifunction Devices" (Come aggiornare, dotare di patch o clonare i dispositivi multifunzione Xerox) (<http://www.office.xerox.com/support/dctips/dc06cc0410.pdf>)

Metodo Software macchina (Aggiornamento)

- 1) Aprire un browser Web e connettersi al dispositivo multifunzione immettendo l'indirizzo IP del dispositivo.
- 2) Selezionare l'icona "Indice" in alto al centro sullo schermo.
- 3) Selezionare "Software macchina (Aggiornamenti)".
- 4) Inserire il nome utente e la password del dispositivo.
- 5) In "Manual Upgrade" (Aggiornamento manuale), selezionare il pulsante Browse (Sfoglia) per individuare e poi selezionare il file **WCP275_WC7665_P32v2.dlm**.
- 6) Premere il pulsante "Install Software" (Installa software).
- 7) A questo punto, tutti i sistemi WCP stamperanno un foglio di installazione della patch e poi si riavvieranno automaticamente per installare la patch. Quando **.P32v2** viene aggiunto al numero di versione del controller di rete (ESS), significa che la patch è installata.

Appendice A - Come ottenere il software di sistema

Per ottenere le versioni *.60.22.000 (o successive) del software di sistema:

- a) Aprire un browser Web per accedere al sito www.xerox.com.
- b) Selezionare il collegamento "Supporto e Driver".
- c) Selezionare "Multifunzione".
- d) In base al modello che si possiede, selezionare "WorkCentre" o "WorkCentre Pro".
- e) Individuare il collegamento che corrisponde al proprio modello di WorkCentre.
- f) Selezionare "Driver e Download".
- g) Selezionare il collegamento "Aggiornamenti per i prodotti".
- h) Selezionare il collegamento "System software set *.60.22.000 Install Instructions" e stampare il documento (oppure salvarlo).
- i) Selezionare il collegamento per "System Software set *.60.22.000" e salvare il file sul computer.
- j) Dopo aver scaricato il file, estrarne il contenuto sul desktop.
- k) Consultare il file delle istruzioni per l'installazione del software di sistema ("System Software Install Instructions") salvato prima.
- l) Eseguire l'aggiornamento del dispositivo.

Appendice B – Abilitazione di LPD (stampa dalla porta 515)

Per poter utilizzare il metodo LPR per applicare la patch, è necessario che il dispositivo multifunzione supporti la stampa LPD (Line Printer Daemon) mediante la porta 515. Nella maggior parte dei dispositivi multifunzione, questo protocollo è abilitato per impostazione predefinita. Se la stampa LPD è disabilitata, è necessario abilitarla per poter utilizzare il metodo LPR.

Per abilitare LPD, seguire questi passaggi:

- 1) Aprire un browser Web e connettersi al dispositivo multifunzione immettendo l'indirizzo IP del dispositivo.
- 2) Selezionare l'icona "Indice" o "Indice dispositivi" nella parte superiore dello schermo.
- 3) Selezionare "LPR/LPD" oppure "Line Printer Daemon".
- 4) Se la casella Abilitato NON è selezionata, selezionarla. Apparirà un segno di spunta.
- 5) Selezionare "Applica nuove impostazioni".
- 6) Inserire il nome utente e la password dell'amministratore, quindi selezionare OK.
- 7) Riavviare il dispositivo multifunzione dalla pagina web Stato oppure premere il pulsante di spegnimento del dispositivo.

Declinazione di responsabilità

Le informazioni contenute in questo documento Xerox sono fornite "così come sono" senza alcuna garanzia. Xerox Corporation non riconosce alcuna garanzia, espressa o implicita, comprese le garanzie di commerciabilità e idoneità a uno scopo specifico. In nessun caso Xerox Corporation sarà responsabile di danni di qualsiasi tipo risultanti dall'uso dell'utente o dal mancato rispetto delle informazioni fornite in questo documento Xerox, inclusi senza limitazione danni speciali, diretti, indiretti, incidentali, conseguenti o la perdita di profitti aziendali, anche nel caso in cui Xerox Corporation sia stata informata della possibilità di tali danni. Alcuni paesi non consentono l'esclusione o la limitazione della responsabilità per i danni conseguenti, pertanto le limitazioni di cui sopra potrebbero non essere applicabili.